Ръководство за управление на работния плот

Настолни бизнес устройства

Номер на част на документа: 361202-261

Май 2004

Включва дефиниции и инструкции за използването на функциите за защита и Intelligent Manageability (интелигентна управляемост), които са предварително инсталирани на определени модели.

ПРЕДУПРЕЖДЕНИЕ: Текстът, изложен по този начин, означава, че неизпълнението на упътванията може да доведе до телесни наранявания или смърт.

ВНИМАНИЕ: Текстът, изложен по този начин, означава, че неизпълнението на упътванията може да доведе до повреди на оборудването или загуба на информация.

Ръководство за управление на работния плот
Настолни бизнес устройства

Първо издание (Май 2004)
Номер на част на документа: 361202-261

Съдържание

Ръководство за управление на работния плот

Индекс

Ръководство за управление на работния плот

HP Intelligent Manageability (Интелигентна управляемост на HP) предоставя стандартизирани решения за управление и контролиране на работни плотове, работни станции и лаптопи в в мрежа. HP въвежда управлението на работния плот през 1995 с първите в отрасъла персонални компютри с управляеми работни плотове. HP притежава патента за технологията за управление. От тогава, HP в лидер в разработката на нужните стандарти и инфраструктура за ефективно използване, конфигуриране и управление на работните плотове, работните станции и лаптопите. HP работи заедно с водещи доставчици на услуги и софтуер за управление, за да осигури съвместимост с Intelligent Manageability (Интелигентна управляемост) и тези продукти. Intelligent Manageability (Интелигентна управляемост) е важен аспект от нашия общ ангажимент да ви предоставяме с решения за живота на компютрите, които ви помагат по време на четирите фази – планиране, инсталиране, управление и преход.

Основните възможности и функции на управлението на работен плот са следните:

- Първоначално конфигуриране и инсталиране
- Отдалечено инсталиране на системи
- Актуализация и управление на софтуер
- Промяна на ROM паметта
- Проследяване на активи и защита
- Уведомяване при грешки и възстановяване

Поддръжката на специфични функции, описани в това ръководство, може да се различават според модела или версията на софтуера.

Първоначално конфигуриране и инсталиране

Компютърът се продава с предварително инсталирано копие на системния софтуер. След кратко инсталиране на този софтуер, компютърът е готов за използване.

Може да предпочетете да замените предварително инсталираното копие с персонализиран системен или приложен софтуер. Има няколко метода за инсталирането на персонализирано копие на софтуера. Те са:

- Инсталиране на допълнителни софтуерни приложения след декомпресирането на предварително инсталираното копие на софтуера.
- Използване на инструменти за инсталиране на софтуер, напр. Altiris Deployment Solution™, който да замени предварително инсталирания софтуер с персонализирано копие.
- Използване на процедура за клониране на диска, за да се копира съдържанието от един твърд диск на друг.

Най–добрият метод за инсталиране зависи от съответната среда и процеси. Разделът «PC Deployment» (Инсталиране на PC) в Web сайта «HP Lifecycle Solutions» (http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html) дава информация за това как да изберете най–добрия метод за инсталиране.

Компактдискът *Restore Plus!* ROM–базираното инсталиране, и ACPI хардуерът предоставят още помощ при възстановяването на системния софтуер, управлението на конфигурацията, отстраняването на неизправности и управлението на електроенергията.

Отдалечено инсталиране на системи

Отдалеченото инсталиране на системите ви позволява да започнете и инсталирате системата с помощта на софтуера и конфигурационната информация на мрежов сървър със стартиране на Preboot Execution Environment (PXE) (Среда за изпълнение преди стартиране). Функцията «Отдалечени инсталиране на системи» обикновено се използва като инструмент за инсталиране и конфигуриране и може да се използва за следните задачи:

- Форматиране на твърд диск
- Инсталиране на копие на софтуер на един или повече нови компютри
- Отдалечено актуализиране на системния BIOS във ROM флаш паметта («Отдалечена ROM флаш памет» на стр. 8)
- Конфигуриране на настройките в BIOS

За да стартирате Remote System Installation (Отдалечено инсталиране на системи), натиснете **F12** когато в долния десен ъгъл на екрана с емблемата на HP се появи съобщението F12 = Network Service Boot (F12 = Стартиране от мрежа). Следвайте инструкциите на екрана, за да продължите. Редът на стартиране по подразбиране е настройка в BIOS, която може да се промени така, че винаги PXE стартирането да е активно.

HP и Altiris имат споразумение да предоставят инструменти, предназначени за улесняване на корпоративното инсталиране и управление на компютри, както и намаляване на нужното време за това, като по този начин драстично се намалят разходите и компютрите на HP се превърнат в най–лесно управляемите от всички останали в една корпоративна среда.

Актуализация и управление на софтуер

HP предоставя няколко инструмента за управление и актуализация на софтуера на настолни и работни станции– HP Client Manager Software, Altiris Client Management Solutions, System Software Manager; Proactive Change Notification и Subscriber's Choice.

HP Client Manager Software

HP Client Manager Software (HP CMS) помага на клиентите на HP при управлението на хардуера на клиентските компютри с функции като:

- Подробен преглед на хардуера за управление на активите
- Наблюдение и диагностика на компютрите
- Проактивно уведомяване при промени в хардуера
- Достъпни от Интернет отчети на критично важни за бизнеса данни, като компютри с предупреждения за температурата, уведомявания за паметта и др.
- Отдалечено актуализиране на системния софтуер като драйвери и ROM BIOS
- Отдалечена промяна на реда на стартиране

За повече информация за HP Client Manager, посетете http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Client Management Solutions

HP и Altiris има споразумение да предоставят подробни и силно интегрирани решения за системни управление с цел намаляване на разходите по притежаването на компютри на HP. HP Client Manager Software е основата за допълнителни решения от Altiris Client Management които се отнасят за:

- Управление на инвентара и активите
  - ❏ Съвместимост със софтуерни лицензи
  - ❏ Проследяване на компютри и отчет
  - ❏ Договори за лизинг, проследяване на фиксирани активи

- Инсталиране и мигриране
  - Мигриране на Microsoft Windows XP Professional или Home Edition
  - Инсталиране на системата
  - Мигриране на личността
- Бюро за поддръжка и решение на проблеми
  - Управление на билети от бюрото за поддръжка
  - Отдалечено отстраняване на неизправности
  - Отдалечено решение на проблеми
  - Възстановяване на проблеми при клиенти
- Управление на софтуер и операции
  - Постоянно управление на работния плот
  - Инсталиране на системния софтуер на HP
  - Самокоригиране на приложения

За повече информация и подробности как да изтеглите напълно функционална 30–дневна пробна версия на решенията на Altiris, посетете http://h18000.www1.hp.com/im/prodinfo.html#deploy.

При определени настолни и преносими компютърни модели агентът за управление на Altiris е включен като част от фабрично зареденото копие. Този агент разрешава комуникацията с Altiris Development Solution, който може да се използва за завършване на инсталирането на нов хардуер или мигриране на личности на нова операционна система с помощта на лесни за използване съветници. Решенията на Altiris ви дават лесни за използване възможности за разпространяване на софтуера. Когато се използва заедно с System Software Manager или HP Client Manager Software, администраторите могат също така да актуализират ROM BIOS и драйверите от централна конзола.

За повече информация, посетете http://h18000.www1.hp.com/im/index.html.

System Software Manager

System Software Manager (SSM) е помощна програма, която ви позволява едновременно да актуализирате системен софтуер на няколко системи. Когато се стартира на клиентски компютър, SSM открива версиите на хардуера и софтуера, след което актуализира съответния софтуер от централизирано място, което се нарича хранилище на файлове. Версиите на драйвери, които се поддържат от SSM са отбелязани със специална икона в Web сайта за изтегляне на драйвери, както и на Support Software CD (Компактдиск за поддръжка). За да изтеглите помощната програма или да получите повече информация за SSM, посетете http://www.hp.com/go/ssm.

Проактивно уведомяване при промени

Програмата Proactive Change Notification (Проактивно уведомяване при промени) използва Web сайта Subscriber's Choice, за да прави автоматично следните неща:

- Да ви изпраща PCN e–mail съобщения, които ви уведомяват за промени в хардуера и софтуера на повечето търговски компютри и сървъри, до 60 дни предварително.
- Да ви изпраща e–mail съобщения с бюлетини за клиенти, за защитата, бележки и уведомявания за драйвери за повечето търговски компютри и сървъри.

Вие създавате ваш собствен профил, за да сте сигурни, че само вие получавате информацията за определена ИТ среда. За да научите повече за тази програма и да създадете профил по избор, посетете http://h30046.www3.hp.com/subhub.php?jumpid=go/pcn.

Subscriber's Choice (Избор на абоната)

Subscriber's Choice (Избор на абоната) е услуга от HP, базирана на клиенти. На базата на вашия профил, HP ще ви предоставя персонализирани съвети за продукти, актуални статии и/или уведомявания/предупреждения за поддръжка и драйвери. Subscriber's Choice Driver и Support Alerts/Notifications (Драйвер на абоната и уведомявания/предупреждения за поддръжка) ще изпращат e–mail съобщения, с които да ви уведомят, че информацията, за която сте се абонирали в профила си е налична за преглед и изтегляне. За да научите повече за Subscriber's Choice (Избор на абоната) и да създадете профил по избор, посетете http://h30046.www3.hp.com/subhub.php.

ROM флаш памет

Компютърът е с програмируема ROM (непроменлива) флаш памет. Като зададете парола за настройка в Computer Setup (Помощна програма), можете да защитите ROM паметта от неоторизирано актуализизиране или презаписване. Това е важно са подсигуряването на защитата на компютъра. Ако се наложи да надстройвате ROM паметта, можете да:

- Поръчате нова ROMPaq дискета от HP.
- Изтеглите последните ROMPaq копия от страницата за драйвери и поддръжка на HP http://www.hp.com/support/files.

ВНИМАНИЕ: За максимална защита ROM паметта задайте парола за настройка. Паролата за настройка предотвратява неоторизирана надстройка на ROM паметта. System Software Manager (Диспечер на системния софтуер) позволява на системния администратор да зададе парола за настройка на един или повече компютри наведнъж. За още информация посетете http://www.hp.com/go/ssm.

Отдалечена ROM флаш памет

Отдалечената ROM флаш памет позволява на системните администратори спокойно да актуализират ROM паметта на отдалечени компютри на HP направо от централизиране конзола за управление на мрежата. Тази възможност за изпълнение на задачата от далеч и на много компютри наведнъж, позволява постоянно използване и по−голям контрол върху PC ROM копията на HP в мрежата. Това също увеличава продуктивността и намалява разходите.

Компютърът трябва да е включен от бутона за захранване или чрез Remote Wakeup (Отдалечно включване), за да се използва Remote ROM Flash (Отдалечена ROM флаш памет).

За повече информация за Remote ROM Flash (Отдалечно включване), вж. HP Client Manager Software или System Software Manager на адрес http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

Помощната програма HPQFlash се използва за актуализиране и възстановяване на системната ROM памет на отделни компютри чрез операционната система Windows.

За повече информация за HPQFlash, посетете http://www.hp.com/support/files и въведете името на компютъра като се появи съобщението.

FailSafe Boot Block ROM (FailSafe блокиране на ROM паметта при стартиране)

FailSafe Boot Block ROM позволява възстановяването на системата в редки случаи на проблем при актуализацията на ROM паметта, например ако токът спре по време на актуализацията на ROM паметта. Boot Block (Блок за стартиране) е защитена част от ROM паметта, която проверява дали има валидна системна ROM памет при включване на компютъра.

- Ако системната ROM памет в валидна, системата стартира нормално.
- Ако системната ROM памет не е валидна, FailSafe Boot Block ROM предоставя поддръжка за стартирането на системата от ROMPaq дискета, която програмира системната ROM памет с валидно копие.

При някои модели се поддържа възстановяване от ROMPaq компактдиск. ISO ROMPaq копията са включени към определени модели в ROM пакети за изтегляне.

Когато блокът за стартиране открие невалидна системна ROM памет, индикаторът за захранване мига осем пъти, един път на секунда през две секунди. Ще се чуят и осем звука. На екрана ще се появи съобщение за възстановяване от блока за стартиране (при някои модели).

За да възстановите системата след като тя навлезе в режим на възстановяване чрез блока за стартиране, изпълнете следните стъпки:

1. Ако има носител във флопидисковото или CD–ROM устройството, извадете го и изключете захранването.
2. Поставете ROMPaq дискета в устройството, или, ако е възможно ROMPaq компактдиск в устройството.
3. Включете компютъра.

   Ако няма ROMPaq дискета или диск, ще се появи съобщение да поставите и да рестартирате компютъра.

   Ако е зададена парола за настройка, индикаторът за главни букви ще светне и ще се появи съобщение да въведете парола.
4. Въведете паролата за настройка.

   Ако системата стартира успешно от дискетата и препрограмира ROM паметта, ще светнат и трите индикатора на клавиатурата. Ще се чуе и серия от увеличаващи се сигнали.
5. Извадете дискетата или диска и изключете захранването.
6. Включете захранването и рестартирайте компютъра.

Следната таблица съдържа различни комбинации на индикаторите на клавиатурата, които се използват от Boot Block ROM паметта (ако клавиатурата е PS/2) и обяснява значението и съответните действия при всяка комбинация.

Комбинации на индикаторите на клавиатурата, използвани от Boot Block ROM паметта

Режим FailSafe Boot Block ROM (FailSafe блокиране на ROM паметта при стартиране)	Цвят на индикатора на клавиатурата	Клавиатура Активност на индикатора	Състояние/ съобщение
Num Lock	Зелено	On (Включено)	Няма ROMPaq дискета или диск, те са повредени или устройството не е готово.
Caps Lock	Зелено	On (Включено)	Въведете парола.
Num, Caps, Scroll Lock	Зелено	Поредица от мигане, всички по веднъж – N, C, SL	Клавиатурата е заключена в мрежов режим.
Num, Caps, Scroll Lock	Зелено	On (Включено)	Успешна е актуализацията на Boot Block ROM паметта. Изключете и включете захранването, за да рестартирате.

✎ Индикаторите за диагностика не мигат при USB клавиатури.

Копиране на настройките

Следните процедури дават на администраторите възможност лесно да копират настройките на една конфигурация на друга при едни и същи модели. Така конфигурацията на много компютри е по–постоянна и по–бърза.

И двете процедури изискват флопидисково устройство или поддържано USB устройство за носители с флаш памет, като например HP Drive Key.

Копиране на един компютър

ВНИМАНИЕ: Всяка конфигурация на настройките е специфична за модела. Файловата система може да се повреди ако компютрите не са един и същ модел. Например, не копирайте настройките от dc7100 Ultra–Slim Desktop на dx6100 Slim Tower.

1. Изберете конфигурация за копиране. Изключете компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Shut Down (Изключване)**.
2. Ако използвате USB устройство с флаш памет, поставете го сега.
3. Включете компютъра.
4. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

5. Ако използвате дискета я поставете.

6. Щракнете върху **File (Файл) > Replicated Setup (Копирани настройки) > Save to Removable Media (Запиши на сменяем носител)**. Следвайте инструкциите на екрана, за да създадете дискетата или USB флаш устройството с конфигурацията.
7. Изключете компютъра, който конфигурирате и поставете дискетата или USB флаш устройството с конфигурацията.
8. Включете компютъра, който ще конфигурирате.
9. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.
10. Щракнете върху **File (Файл) > Replicated Setup (Копирани настройки) > Restore from Removable Media (Възстанови от сменяемия носител)** и следвайте инструкциите на екрана.
11. Рестартирайте компютъра, когато конфигурацията завърши.

Копиране на много компютри

ВНИМАНИЕ: Всяка конфигурация на настройките е специфична за модела. Файловата система може да се повреди ако компютрите не са един и същ модел. Например, не копирайте настройките от dc7100 Ultra–Slim Desktop на dx6100 Slim Tower.

Този метод отнема повече време за подготовката на дискетата или USB флаш устройството с конфигурацията, но копирането на останалите компютри и значително по–бързо.

За тази процедура е нужна стартираща дискета или създаването на стартиращо USB флаш устройство. Ако нямате Windows XP, за да създадете стартираща дискета, използвайте метода за копиране на един компютър (вж. «Копиране на един компютър» на стр. 11).

1. Създайте стартираща дискета или USB флаш устройство. Вж. «Поддържано USB флаш устройство» на стр. 14, или «Неподдържано USB флаш устройство» на стр. 17.

ВНИМАНИЕ: Не всички компютри могат да стартират от USB флаш устройство. Ако редът на стартиране в Computer Setup показва USB устройство като възможност, компютърът може да стартира от USB флаш устройство. В противен случай трябва да се използва стартираща дискета.

2. Изберете конфигурация за копиране. Изключете компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Shut Down (Изключване)**.
3. Ако използвате USB устройство с флаш памет, поставете го сега.
4. Включете компютъра.
5. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

6. Ако използвате дискета я поставете.
7. Щракнете върху **File (Файл) > Replicated Setup (Копирани настройки)** Следвайте инструкциите на екрана, за да създадете дискетата или USB флаш устройството с конфигурацията.
8. Изтеглете BIOS програмата за копиране на настройките (repset.exe) и я копирайте на дискетата или USB флаш устройството с конфигурацията. За да получите тази програма, посетете http://welcome.hp.com/support/files и въведете номера на модела на компютъра.
9. Върху дискетата или USB флаш устройството създайте файл autoexec.bat със следната команда:

   repset.exe

10. Изключете компютъра, който ще конфигурирате. Поставете дискетата или USB флаш устройството и включете компютъра. Програмата за конфигуриране автоматично ще стартира.
11. Рестартирайте компютъра, когато конфигурацията завърши.

Създаване на стартиращо устройство

Поддържано USB флаш устройство

Поддържаните устройства, като HP Drive Key или DiskOnKey, имат предварително инсталирано копие, за да се опрости процес на превръщането им в стартиращи. Ако използваното USB флаш устройство няма такова копие, използвайте процедурата, описана по–надолу в този раздел (вж. «Неподдържано USB флаш устройство» на стр. 17).

ВНИМАНИЕ: Не всички компютри могат да стартират от USB флаш устройство. Ако редът на стартиране в Computer Setup показва USB устройство като възможност, компютърът може да стартира от USB флаш устройство. В противен случай трябва да се използва стартираща дискета.

За да създадете стартиращо USB флаш устройство, трябва да имате:

- Една от следните системи:
  - HP Compaq Business Desktop dc7100 series
  - HP Compaq Business Desktop dx6100 series
  - HP Compaq Business Desktop d530 Series – Ultra–Slim Desktop, Small Form Factor или Convertible Minitower
  - Compaq Evo D510 Ultra–slim Desktop
  - Compaq Evo D510 Convertible Minitower/Small Form Factor

  В зависимост от BIOS, бъдещите системи може също да поддържат стартиране от USB флаш устройство.

ВНИМАНИЕ: Ако използвате компютър, различен от указаните по–горе, уверете се, че редът на стартиране в Computer Setup показва USB устройството преди твърдия диск.

- Един от следните модули за съхранение:
  - 16MB HP Drive Key
  - 32MB HP Drive Key
  - 32MB DiskOnKey
  - 64MB HP Drive Key
  - 64MB DiskOnKey
  - 128MB HP Drive Key
  - 128MB DiskOnKey
  - 256MB HP Drive Key
  - 256MB DiskOnKey
- Стартираща дискета с DOS с програмите FDISK и SYS. Ако SYS я няма, може да се използва FORMAT, но всички файлове на USB флаш устройството ще се изтрият.

1. Изключете компютъра.
2. Включете USB флаш устройството в един от USB портовете на компютъра и изключете всички останали USB устройства за съхранение без USB флопидисковите.
3. Поставете стартираща дискета с DOS с програмите FDISK.COM и или SYS.COM или FORMAT.COM и включете компютъра, за да стартира от дискетата.
4. Изпълнете FDISK от A:\ prompt като въведете **FDISK** и натиснете Enter. Ако се появи съобщение, натиснете **Yes (Да)** (**Y**), за да разрешите поддръжка на големи дискове.
5. Въведете избор [**5**], за да се покажат устройствата в системата. USB флаш устройството, чийто размер донякъде съответства на едно показаните. Това обикновено е последното устройство от списъка. Отбележете буквата на устройството.

   USB флаш устройство: _____

ВНИМАНИЕ: Ако в дадено устройство не може да се постави USB флаш устройство, не продължавайте. Може да се изтрият данни. Проверете всички останали USB портове за допълнителни устройства за съхранение. Ако има такива ги изключете, рестартирайте компютъра и продължете към стъпка 4. Ако няма, системата не поддържа USB флаш устройството или то е повредено. НЕ правете USB флаш устройството стартиращо.

6. Излезте от FDISK като натиснете клавиша **Esc**, за да се върнете към A:\.
7. Ако на стартиращата дискета има SYS.COM, преминете към стъпка 8. Ако не, към стъпка 9.
8. На A:\ prompt въведете **SYS x:** където x е буквата на устройството.

ВНИМАНИЕ: Уверете се, че сте въвели правилната буква за USB флаш устройството.

След прехвърлянето на системните файлове, SYS ще се върне на реда A:\. Преминете към стъпка 13.

9. Копирайте файловете от USB флаш устройството, които искате да запазите, във временна директория на друго устройство (например, твърдия диск на системата).
10. В A:\ prompt, въведете **FORMAT /S X:** където X е буквата на устройството.

ВНИМАНИЕ: Уверете се, че сте въвели правилната буква за USB флаш устройството.

FORMAT ще покаже едно или няколко съобщения, които ви питат дали искате да продължите. Въведете **Y** всеки път. FORMAT ще форматира USB флаш устройството, ще добави системни файлове и ще попита за етикет на диска.

11. Натиснете клавиша **Enter** ако не искате етикет или въведете такъв.
12. Копирайте записаните файлове от стъпка 9 обратно в USB флаш устройството.

13. Извадете дискетата и рестартирайте компютъра. Компютърът ще се рестартира с USB флаш устройството, което ще е с буквата C.

Редът на стартиране е различен при различните компютри и може да се промени в Computer Setup (Настройка на компютъра).

Ако сте използвали DOS версия от Windows 9x, може да се появи екран с емблемата на Windows. Ако не искате този екран, добавете файл с нулев размер LOGO.SYS в главната директория на USB флаш устройството.

Върнете се към «Копиране на много компютри» на стр. 12.

Неподдържано USB флаш устройство

ВНИМАНИЕ: Не всички компютри могат да стартират от USB флаш устройство. Ако редът на стартиране в Computer Setup показва USB устройство като възможност, компютърът може да стартира от USB флаш устройство. В противен случай трябва да се използва стартираща дискета.

За да създадете стартиращо USB флаш устройство, трябва да имате:

- Една от следните системи:
  - HP Compaq Business Desktop dc7100 series
  - HP Compaq Business Desktop dx6100 series
  - HP Compaq Business Desktop d530 Series – Ultra–Slim Desktop, Small Form Factor или Convertible Minitower
  - Compaq Evo D510 Ultra–Slim Desktop
  - Compaq Evo D510 Convertible Minitower/Small Form Factor

  В зависимост от BIOS, бъдещите системи може също да поддържат стартиране от USB флаш устройство.

ВНИМАНИЕ: Ако използвате компютър, различен от указаните по–горе, уверете се, че редът на стартиране в Computer Setup показва USB устройството преди твърдия диск.

- Стартираща дискета с DOS с програмите FDISK и SYS. Ако SYS я няма, може да се използва FORMAT, но всички файлове на USB флаш устройството ще се изтрият.

1. Ако в системата има PCI платки, които имат прикрепени SCSI, ATA RAID или SATA устройства, изключете компютъра и извадете кабела от контакта.

ВНИМАНИЕ: Кабелът за захранване ТРЯБВА да е изключен.

2. Отворете компютъра и извадете PCI платките.
3. Включете USB флаш устройството в един от USB портовете на компютъра и изключете всички останали USB устройства за съхранение без USB флопидисковите. Затворете капака на компютъра.
4. Включете кабела и компютъра.
5. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

6. Отидете на **Advanced (Разширени) > PCI Devices (PCI устройства)**, за да забраните PATA и SATA контролерите. При забраняването на SATA контролера, отбележете IRQ, което се задава на контролера. По–късно ще трябва отново да зададете IRQ. Излезте от програмата като потвърдите промените.

   SATA IRQ: _____

7. Поставете стартираща дискета с DOS с програмите FDISK.COM и или SYS.COM или FORMAT.COM и включете компютъра, за да стартира от дискетата.

8. Изпълнете FDISK и изтрийте съществуващите дялове на USB флаш устройството. Създайте нов дял и го маркирайте като активен. Излезте от FDISK като натиснете клавиша **Esc**.
9. Ако системата не стартира автоматично при изход от FDISK, натиснете **Ctrl+Alt+Del**, за рестарт от дискетата с DOS.
10. В A:\ prompt, въведете **FORMAT C: /S** и натиснете клавиша **Enter**. Format ще форматира USB флаш устройството, ще добави системни файлове и ще попита за етикет на диска.
11. Натиснете клавиша **Enter** ако не искате етикет или въведете такъв.
12. Изключете компютъра и извадете щепсела от контакта. Отворете компютъра и отново инсталирайте PCI платките, които сте извадили преди това. Затворете капака на компютъра.
13. Включете кабела за захранване на компютъра, извадете дискетата и включете компютъра.
14. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.
15. Отидете на to **Advanced (Разширени) > PCI Devices (PCI устройства)** и отново разрешете PATA и SATA контролерите, които забранихте в стъпка 6. Задайте първоначалното IRQ на SATA контролера.
16. Запишете промените и излезте. Компютърът ще се рестартира с USB флаш устройството, което ще е с буквата C.

Редът на стартиране е различен при различните компютри и може да се промени в Computer Setup (Настройка на компютъра). Вж. *Computer Setup Guide (Ръководство за настройка на компютъра)* в *компактдиска с документация* за инструкции.

Ако сте използвали DOS версия от Windows 9x, може да се появи екран с емблемата на Windows. Ако не искате този екран, добавете файл с нулев размер LOGO.SYS в главната директория на USB флаш устройството.

Върнете се към «Копиране на много компютри» на стр. 12.

Бутон за захранване в двойно състояние

Ако Advanced Configuration and Power Interface (Интерфейс за разширена конфигурация и електроенергия) е разрешен, бутонът за захранване може да функционира като бутона за вкл./изкл. или като бутон за режим на готовност. Функцията за режим на готовност не изключва изцяло компютъра, а превключва в режим на готовност с ниско енергопотребление. Това ви позволява бързо да изключвате компютъра без да затваряте приложения и после бързо да се върнете към тях без да губите никакви данни.

За да промените конфигурацията на бутона за захранване, изпълнете следните стъпки:

1. Щракнете с ляв бутон върху бутона **Start (Старт)**, изберете **Control Panel (Контролен панел) > Power Options (Опции за електроенергия)**.
2. В **Power Options Properties (Свойства на опциите за електроенергия)**, изберете раздела **Advanced (Разширени)**.
3. В раздела **Power Button (Бутон за захранване)** изберете **Stand by (Готовност)**.

След като конфигурирате бутона за захранване да работи като бутона за състояние на готовност, натиснете го за да може компютърът да превключи на този режим. Натиснете бутона пак за бързо превключване в нормален режим. За да изключите изцяло захранването от компютъра, натиснете и задръжте бутона за четири секунди.

ВНИМАНИЕ: Не използвайте бутона за захранване за изключване на системата, освен ако тя е блокирала; изключването без помощта на операционната система може да повреди или изтрие данни от твърдия диск.

Web сайт

Инженерите на HP полагат усилия за тестването и отстраняването на неизправности в разработен от HP софтуер, както и от трети доставчици. Те разработват специфичен софтуер за поддръжка на операционни системи, за да гарантират производителността, съвместимостта и надеждността за всички компютри на HP.

Когато преминавате на нова или актуализирана операционна система, важно е този софтуер за съответната операционна система да се използва. Ако възнамерявате да работите с версия на Microsoft Windows, която е различна от включената към компютъра, трябва да инсталирате съответните драйвери и помощни програми, за да сте сигурни, че всички функции се поддържат и работят правилно.

HP е улеснил процедурата за намиране, достъп, оценка и инсталиране на най–новия софтуер. Можете да изтеглите софтуера от http://www.hp.com/support.

Web сайтът съдържа последните драйвери, помощни програми и ROM копия, които трябват, за да работи Microsoft Windows operating на компютър на HP.

Разработчици и партньори

Решенията за управление на HP се интегрират с други приложения за системно управление и се базират на индустриални стандарти като:

- Web–базирано корпоративно управление (WBEM)
- Интерфейс за управление на Windows (WMI)
- Технология «Wake on LAN»
- ACPI
- SMBIOS
- Поддръжка на изпълнение преди стартиране (Pre–boot Execution)

Проследяване на активи и защита

Вградените в компютъра функции за проследяване на активи предоставят ключови данни за активите, които могат да се управляват с помощта на HP Systems Insight Manager, HP Client Manager или други подобни приложения за системно управление. Безупречното интегриране между тези функции за проследяване на активи и продуктите ви позволяват да изберете инструмента за управление, който е най–подходящ за съответната среда и съответно да регулирате инвестициите в съществуващи инструменти.

HP също така предлага няколко решения за контролиране на достъпа до ценни компоненти и информация. Ако е инсталиран ProtectTools Embedded Security, той предотвратява неоторизиран достъп до данни и проверява системата, като удостоверява трети потребители, които се опитват да получат достъп до системата. (Вж. *Getting Started (Начални стъпки), HP ProtectTools Embedded Security Manager,* в *компактдиска с документация* за повече информация.) Функциите за защита, като ProtectTools, ключалката и сензорът на интелигентния капак, налични при определени модели, помагат за предотвратяването на неоторизиран достъп до вътрешните компоненти на компютъра. Като забраните паралелните, серийните или USB портовете, или възможността за стартиране от сменям носител, можете да защитите ценни активи на данни. Уведомяванията за смяна на памет или от сензора на интелигентния капак може автоматично да се препращат към приложения за системно управление за проактивно уведомяване при достъп до вътрешните компоненти на компютъра.

Инструменти за защита, сензор на интелигентния капак и ключалката на интелигентния капак са налични като опции при определени модели.

Използвайте следните помощни програми, за да управлявате настройките за защита на компютъра на HP:

- На място, с помощта на Computer Setup (Настройка на компютъра). Вж. *Computer Setup (F10) Utility Guide (Помощно ръководство за настройка на компютъра)* в *компактдиска с документация* към компютъра за допълнителна информация и инструкции за използването на помощните програми на Computer Setup (Настройка на компютъра).
- Отдалечено използване на HP Client Manager Software или System Software Manager. Този софтуер ви позволява безопасно и постоянно използване и контрол на настройките за защита от програма в команден ред.

Следната таблица и раздели се отнасят за функции за управление на защитата локално на компютъра чрез програмите на Computer Setup (Настройка на компютъра).

Преглед на функциите за защита

Опция	Описание
Setup Password (Парола за настройки)	Позволява ви да въведете и активирате парола за настройки (администратора). ✎ Ако е зададена парола за настройки, тя ще се изисква при промяната на опции в Computer Setup, изтриване на ROM паметта и промяната на някои опции тип Plug & Play в Windows. Вж. *Troubleshooting Guide (Ръководство за отстраняване на неизправности)* в *компактдиска «Документация»* за повече информация.
Power–On Password (Парола при включване на захранването)	Позволява ви да въведете и активирате парола при включване на захранването. Вж. *Troubleshooting Guide (Ръководство за отстраняване на неизправности)* в *компактдиска «Документация»* за повече информация.

✎ За повече информация за Computer Setup (Настройка на компютъра), вж. *Computer Setup (F10) Utility Guide (Помощно ръководство за настройка на компютъра)* в *компактдиска с документация*.

Поддръжката на функциите за защита зависят от специфичната конфигурация.

Преглед на функциите за защита *(продължение)*

Опция	Описание
Password Options (Опции за парола) (Тази възможност за избор ще се появи само ако е зададена парола при включване на захранването.)	Позволява ви да укажете дали паролата да се изисква при «топло рестартиране» (**CTRL**+**ALT**+**DEL**). Вж. *Desktop Management Guide (Ръководство за управление на работния плот)* в *компактдиска «Документация»* за повече информация.
Pre–Boot Authorization (Оторизация преди стартиране)	Позволява ви да разрешите/забраните използването на смарткарта вместо парола при включване на захранването.
Интелигентен капак	Позволява ви да: • Разрешите/забраните ключалката на капака. • Разрешите/забраните сензора за сваляне на капака. ✎ *Notify User (Уведомяване на потребителя)* уведомява потребителя, че сензорът е засякъл отваряне на капака. *Setup Password (Парола за настройка)* изисква въвеждането на парола при стартирането на компютъра, ако сензорът засече отваряне на капака. Тази функция се поддържа само при определени модели. Вж. *Desktop Management Guide (Ръководство за управление на работния плот)* в *компактдиска «Документация»* за повече информация.
Embedded Security (Вградена защита)	Позволява ви да: • Разрешите/забраните устройството с вградена защита. • Възстановите фабричните настройки на устройството. Тази функция се поддържа само при определени модели. Вж. *Ръководството за вградена защита на HP ProtectTools* на *Компактдиска с документация* за повече информация.
Device Security (Защита на устройствата)	Разрешава/забранява серийните портове, паралелния порт, предните USB портове, звука на системата, мрежовите платки (при някои модели), MultiBay устройствата (при някои модели) и SCSI контролерите (при някои модели).

✎ За повече информация за Computer Setup (Настройка на компютъра), вж. *Computer Setup (F10) Utility Guide (Помощно ръководство за настройка на компютъра)* в *компактдиска с документация*.

Поддръжката на функциите за защита зависят от специфичната конфигурация.

Преглед на функциите за защита *(продължение)*

Опция	Описание
Network Service Boot (Стартиране от мрежа)	Разрешава/забранява възможността на компютъра да стартира от операционна система, инсталирана на мрежов сървър. (Тази функция е налична само при моделите с мрежови платки; мрежовата платка трябва да е поставена в PCI гнездото или да е вградена на дънната платка.)
System IDs (Системни идентификатори)	Позволяват ви да: • Етикет за актив (18–байтов идентификатор) и Етикет за актив (80–байтов идентификатор, който се показва при POST). Вж. *Desktop Management Guide (Ръководство за управление на работния плот* в *компактдиска «Документация»* за повече информация. • Серийният номер на шасито или универсалният уникален идентификатор (UUID). UUID може да се промени само ако серийният номер на шасито е невалиден. (Тези идентификатори обикновено се задават фабрично и се използват за идентифицирането на всяка една система.) Клавиатурната настройка за езика (напр. английска или немска) за записа на системния идентификатор.

✎ За повече информация за Computer Setup (Настройка на компютъра), вж. *Computer Setup (F10) Utility Guide (Помощно ръководство за настройка на компютъра)* в *компактдиска с документация*.

Поддръжката на функциите за защита зависят от специфичната конфигурация.

Преглед на функциите за защита *(продължение)*

Опция	Описание
DriveLock (Заключване на устройства)	Позволява ви да зададете или промените главна или потребителска парола за MultiBay твърди дискове (не се поддържа при SCSI твърди дискове). Когато тази функция е разрешена, по време на POST излиза съобщение за въвеждане на една от потребителските пароли. Ако нито една от тях не се въведе правилно, твърдият диск няма да може да се използва, докато не се въведе правилната парола при следващи «студени рестартирания» на компютъра. ✎ Тази възможност за избор ще се появи само когато в системата е инсталирано поне едно MultiBay устройство, което поддържа функцията DriveLock. Вж. *Desktop Management Guide (Ръководство за управление на работния плот)* в *компактдиска «Документация»* за повече информация.

✎ За повече информация за Computer Setup (Настройка на компютъра), вж. *Computer Setup (F10) Utility Guide (Помощно ръководство за настройка на компютъра)* в *компактдиска с документация*.

Поддръжката на функциите за защита зависят от специфичната конфигурация.

Преглед на функциите за защита *(продължение)*

Опция	Описание
Master Boot Record Security (Защита на главния сектор за стартиране)	Позволява ви да разрешите или забраните Master Boot Record Security (Защита на главния сектор за стартиране). Ако опцията е разрешена, BIOS ще отхвърля всички заявки за запис върху MBR сектора на текущия стартиращ диск. При всяко включване или рестартиране на компютъра, BIOS сравнява MBR сектора на текущия стартиращ диск с този, който е записан преди това. Ако има промени, имате възможност да запишете MBR сектора на текущия стартиращ диск, да възстановите предишно записания или да забраните защитата на MBR. Трябва да знаете главната парола, ако има такава. ✎ Забранете защитата на MBR, преди да форматирате или разделяте текущия стартиращ диск. Няколко помощни дискови програми (като FDISK и FORMAT) искат достъп за промяна на MBR сектора. Ако е разрешена защитата на MBR сектора и достъпът до дисковете се управлява от BIOS, заявките за запис върху MBR сектора се отхвърлят, което кара съответните помощни програми да показват съобщения за грешка. Ако защитата на MBR сектора е разрешена и достъпът до дисковете се управлява от операционната система, направените промени в MBR сектора ще бъдат открити от BIOS при следващото рестартиране и ще се покаже предупредително съобщение за защита на MBR сектора.
Save Master Boot Record (Запиши главния сектор за стартиране)	Записва архивно копие на главния сектор за стартиране върху текущия стартиращ диск. Показва се само ако е разрешена защита на MBR сектора.

✎ За повече информация за Computer Setup (Настройка на компютъра), вж. *Computer Setup (F10) Utility Guide (Помощно ръководство за настройка на компютъра)* в *компактдиска с документация*.

Поддръжката на функциите за защита зависят от специфичната конфигурация.

Преглед на функциите за защита *(продължение)*

Опция	Описание
Restore Master Boot Record (Възстанови главния сектор за стартиране)	Възстановява записания главен сектор за стартиране от текущия стартиращ диск. ✎ Показва се само ако следните условия са налице: • Разрешена е защита на MBR сектора. • Записано е архивно копие на MBR сектора. • Текущият стартиращ диск е същият, от който е записано архивно копие на MBR сектора. ⚠ **ВНИМАНИЕ:** Възстановяването на записан по–рано MBR сектор, след като помощна дискова програма или операционната програма са променили MBR сектора, може да направи данните върху диска недостъпни. Възстановете записан по–рано MBR сектор само ако сте сигурни, че MBR секторът на текущия стартиращ диск е повреден или заразен от вирус.

✎ За повече информация за Computer Setup (Настройка на компютъра), вж. *Computer Setup (F10) Utility Guide (Помощно ръководство за настройка на компютъра)* в *компактдиска с документация*.

Поддръжката на функциите за защита зависят от специфичната конфигурация.

Защита с парола

Паролата за стартиране предотвратява неоторизираната употреба на компютъра, като въвеждането ѝ се изисква при включване или рестартиране за достъп до приложения или данни. Паролата за настройки предотвратява неоторизирания достъп до Computer Setup (Настройка на компютъра) и може да се използва за нулиране на паролата за включване. Т.е. когато трябва да въведете паролата за включване, въвеждането на паролата за настройки също ще свърши работа.

Може да се зададе парола за настройка за цялата мрежа, за да може системният администратор да се регистрира във всички системи мрежата с цел поддръжка, без да е нужно да знае паролата за включване, дори ако има зададена такава.

Задаване на парола за настройки с Computer Setup (Настройка на компютъра)

Ако системата е с вградено устройство за защита, вж. *Ръководството за вградена защита на HP ProtectTools* на *Компактдиска с документация*. Задаването на парола чрез Computer Setup (Настройка на компютъра) предотвратява преконфигурация на компютъра (използване на Computer Setup (Настройка на компютъра)) докато не се въведе парола.

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Restart (Рестартиране)**.
2. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

---

3. Изберете **Security (Защита)** и след това **Setup Password (Парола за настройки)** и следвайте инструкциите на екрана.
4. Преди да излезете, щракнете върху **File (Файл) > Save Changes and Exit (Запис на настройките и изход)**.

Задаване на парола за включване с помощта на Computer Setup (Настройка на компютъра)

Задаването на парола за включване чрез Computer Setup (Настройка на компютъра) предотвратява достъпа до компютъра при включването му, освен ако не се въведе паролата. Когато има зададена парола за включване, в Computer Setup (Настройка на компютъра) има Password Options (Опции за парола) под менюто Security (Защита). Опциите за парола включват Password Prompt on Warm Boot (Съобщение за парола при «топло» включване). Когато Password Prompt on Warm Boot (Съобщение за парола при «топло» включване) е разрешено, паролата трябва да се въвежда при всяко рестартиране на компютъра.

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Restart (Рестартиране)**.
2. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

---

3. Изберете **Security (Защита)** и след това **Power–On Password (Парола за включване)** и следвайте инструкциите на екрана.
4. Преди да излезете, щракнете върху **File (Файл) > Save Changes and Exit (Запис на настройките и изход)**.

Въвеждане на парола за включване

За да въведете парола за включване, изпълнете следните стъпки:

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Restart the Computer (Рестартиране на компютъра)**.
2. Когато на монитора се появи иконата с ключ, въведете текущата парола и натиснете клавиша **Enter**.

Въвеждайте внимателно; знаците не се показват на екрана от съображения за сигурност.

Ако въведете неправилна парола, се показва счупен ключ. Опитайте отново. След три неуспешни опита трябва да изключите компютъра и пак да го включите, за да продължите.

Въвеждане на парола за настройки

Ако системата е с вградено устройство за защита, вж. *Ръководството за вградена защита на HP ProtectTools* на *Компактдиска с документация*.

Ако на компютъра има зададена парола за настройки, ще се показва съобщение за въвеждането ѝ при всеки опит за влизане в Computer Setup (Настройка на компютъра).

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Restart (Рестартиране)**.
2. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

3. Когато на монитора се появи иконата с ключ, въведете паролата за настройки и натиснете клавиша **Enter**.

Въвеждайте внимателно; знаците не се показват на екрана от съображения за сигурност.

Ако въведете неправилна парола, се показва счупен ключ. Опитайте отново. След три неуспешни опита трябва да изключите компютъра и пак да го включите, за да продължите.

Смяна на паролата за настройки или включване

Ако системата е с вградено устройство за защита, вж. *Ръководството за вградена защита на HP ProtectTools* на *Компактдиска с документация*.

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Restart the Computer (Рестартиране на компютъра)**.
2. За да смените паролата за включване, преминете на стъпка 3.

   За да смените паролата за настройки, докато компютърът е включен, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup (Настройка на компютъра). Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

3. Когато се появи иконата с ключ, въведете текущата парола, наклонена черта (/) или подобен разделител, новата парола, още една наклонена черта (/) или подобен разделител и отново новата парола, както е показано: **текуща парола/нова парола/нова парола**

Въвеждайте внимателно; знаците не се показват на екрана от съображения за сигурност.

4. Натиснете клавиша **Enter**.

Новата парола ще е валидна при следващото включване на компютъра.

Вж. «Национални разделители от клавиатурата» на стр. 35 за информация за различни разделители. Паролата за включване и тази за настройки също могат да се сменят с помощта на опциите за защита в Computer Setup (Настройка на компютъра).

Изтриване на паролата за настройки или включване

Ако системата е с вградено устройство за защита, вж. *Ръководството за вградена защита на HP ProtectTools* на *Компактдиска с документация*.

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Restart the Computer (Рестартиране на компютъра)**.
2. За да изтриете паролата за включване, преминете на стъпка 3.

   За да изтриете паролата за настройки, докато компютърът е включен, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup (Настройка на компютъра). Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

---

3. Когато се появи иконата с ключ, въведете текущата парола и след нея наклонена черта (/) или подобен разделител, както е показано:
   текуща парола/
4. Натиснете клавиша **Enter**.

Вж. «Национални разделители от клавиатурата» за информация за различни раделители. Паролата за включване и тази за настройки също могат да се сменят с помощта на опциите за защита в Computer Setup (Настройка на компютъра).

Национални разделители от клавиатурата

Всяка клавиатура е проектирана така, че да отговаря на специфични за съответната страна изисквания. Словоредът и клавишите, които използвате, за да смените или изтриете паролата, зависят от съответната клавиатура.

Национални разделители от клавиатурата

Английски Великобритания	/	Италиански	-	Тайвански	/
Английски САЩ	/	Китайски	/	Тайландски	/
Арабски	/	Корейски	/	Турски	.
Белгийски	=	Латиноамерикански	-	Унгарски	-
Бразилски	/	Немски	-	Френски	!
BHCSY*	-	Норвежки	-	Френско-канадски	é
Гръцки	-	Полски	-	Чешки	-
Датски	-	Португалски	-	Швейцарски	-
Иврит	.	Руски	/	Шведски/ финландски	/
Испански	-	Словашки	-	Японски	/

* За Босна–Херцеговина, Хърватска, Словения и Югославия

Изчистване на пароли

Ако забравите паролата, нямате достъп до компютъра. Вж. *Troubleshooting Guide (Ръководство за отстраняване на неизправности)* в *компактдиска с документация* за повече информация за изчистването на пароли.

Ако системата е с вградено устройство за защита, вж. *Ръководството за вградена защита на HP ProtectTools* на *Компактдиска с документация*.

DriveLock (Заключване на устройства)

DriveLock (Заключване на устройства) стандартна за отрасъла функция за защита, която предотвратява неоторизирания достъп до данни на MultiBay твърди дискове. DriveLock (Заключване на устройства) функционира като допълнение към Computer Setup (Настройка на компютъра). Функцията е налична само при откриване на твърди дискове, които поддържат DriveLock.

DriveLock (Заключване на устройства) е предназначена за клиенти на HP, за които защитата на данните е от изключително значение. За такива клиенти цената на твърдия диск и загубата на данните върху него са несъразмерни с последствията, до които може да се стигне при неоторизиран достъп до тези данни. За да се балансира това ниво на защита с практическата нужда от възможност за възстановяване на забравена парола, схемата на HP DriveLock използва защита с две пароли. Едната парола е предназначена да се задава и използва от системни администратори, а другата от обикновения краен потребител. Няма «задна вратичка», която може да се използва за отключването на диск ако и двете пароли се загубят. Затова функцията DriveLock (Заключване на устройства) се използва най–безопасно, когато данните на твърдия диск се копират на корпоративна информационна система или редовно се архивират.

В случай че и двете пароли за DriveLock бъдат загубени, твърдият диск е практически неизползваем. За потребители, които не влизат в описания по–горе профил, това може да е недопустим риск. За потребители, които влизат в описания по–горе профил на клиенти, това може да е нормален риск, като се има предвид съхранените на твърдия диск данни.

Използване на DriveLock (Заключване на устройства)

Опцията DriveLock се показва под менюто Security (Защита) в Computer Setup (Настройка на коммпютъра). Потребителите имат възможност за зададат главната парола или да разрешат DriveLock. За да се разреши enable DriveLock, трябва да се въведе потребителска парола. Тъй като първоначалната конфигурация на DriveLock (Заключване на устройства) обикновено се изпълнява от системен администратор, трябва първо да се зададе главна парола. HP препоръчва на системните администратори да задават главна парола, независимо дали възнамеряват да разрешат или забранят DriveLock (Заключване на устройства). Така системните администратори ще могат да променят настройките на DriveLock (Заключване на устройства) ако в бъдеще устройството се заключи. След като се зададе главната парола, системният администратор може да разреши или забрани DriveLock (Заключване на устройства).

Ако има заключен твърд диск, при POST ще се изисква парола за отключването му. Ако е зададена парола за включване и тя съвпада с тази на устройството, при POST няма да се изисква повторно въвеждане на паролата. В противен случай ще излезе съобщение за въвеждане на парола за DriveLock (Заключване на устройства). Могат да използват или главената или потребителската парола. Потребителите разполагат с две възможности да въведат правилната парола. Ако опитите им са неуспешни, POST ще продължи, но устройството няма да е достъпно.

Приложения на DriveLock (Заключване на устройства)

Най–практическата употреба на функцията за защита DriveLock (Защита на устройства) е в корпоративна среда, където системният администратор предоставя на потребителите MultiBay твърди дискове за използване с някои компютри. Системният администратор е отговорен за конфигурирането на MultiBay твърди дискове, което освен всичко друго, включва и задаването на главна парола за DriveLock. В случай на забравена парола или ако оборудването се предаде за използване от друг служител, винаги може да се използва главната парола за нулирането на потребителската и да се възстанови достъпа до твърдия диск.

HP препоръчва на корпоративните системни администратори, които решат да разрешат функцията DriveLock (Заключване на устройства), също така да създадат и корпоративни парила за настройка и поддръжка на главни пароли. Това е добре да се прави с цел да се предотвратят ситуации, при които служител умишлено или неумишлено зададе и двете пароли на DriveLock преди да напусне фирмата. При такива случаи, твърдите дискове са неизползваеми и трябва да се сменят. Също така ако не зададат главна парола, системните администратори може да попаднат в ситуация, в която нямат достъп до твърдия диск и да не могат да изпълнят рутинни проверки за неоторизиран софтуер, други функции за контрол на активите и поддръжка.

За потребители с по–малки изисквания за защита, HP не препоръчва разрешаването на функцията DriveLock (Заключване на устройства). Потребителите в тази категория са самостоятелни потребители или такива, които по принцип не държат важни данни на твърдия си диск. За тези потребители потенциалната загуба на твърд диск вследствие на загуба и на двете пароли е много по–голяма от стойността на данните, които функцията DriveLock (Заключване на устройства) е проектирана да пази. Достъпът до Computer Setup (Настройка на компютъра) и функцията DriveLock (Заключване на устройства) може да се ограничи чрез паролата за настройки. Като зададат парола за настройки и не я казват на крайните потребители, системните администратори могат да ограничат разрешаването на функцията DriveLock (Заключване на устройства) от страна на крайните потребители.

Сензор на интелигентния капак

Сензорът за отваряне на капака, наличен при някои модели, е комбинация от хардуерни и софтуерни технологии, които могат да ви уведомяват при отваряне на капака или страничния панел на компютъра. Има три нива на защита, както е описано в следната таблица.

Нива на защита на сензора на интелигентния капак

Ниво	Настройка	Описание
Ниво 0	Забранен	Сензорът на интелигентния капак е забранен (по подразбиране).
Ниво 1	Уведомяване на потребителя	При рестартиране на компютъра на екрана се появява съобщение за това, че е отворен капака или страничния панел на компютъра.
Ниво 2	Setup Password (Парола за настройки)	При рестартиране на компютъра на екрана се появява съобщение за това, че е отворен капака или страничния панел на компютъра. Трябва да въведете паролата за настройки, за да продължите.

✎ Тези настройки могат да се променят с помощта на Computer Setup (Настройка на компютъра). За повече информация за Computer Setup (Настройка на компютъра), вж. *Computer Setup (F10) Utility Guide (Помощно ръководство за настройка на компютъра)* в *компактдиска с документация*.

Настройка на нивото на защита на сензора на интелигентния капак

За да настроите това ниво, изпълнете следните стъпки:

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Restart (Рестартиране)**.
2. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

3. Изберете **Security (Защита) > Smart Cover (Интелигентен капак) > Cover Removal Sensor (Сензор затваряне на капака)** и изберете желаното ниво на защита.
4. Преди да излезете, щракнете върху **File (Файл) > Save Changes and Exit (Запис на настройките и изход)**.

Ключалка на интелигентния капак

Ключалката на интелигентния капак е ключалка за капак, която се управлява от софтуер и е налична при определени компютри на HP. Тази ключалка предотвратява неоторизиран достъп до вътрешните компоненти. Компютърът се продава с незаключена ключалка на интелигентния капак.

ВНИМАНИЕ: За максимална защита с ключалката на капка, задайте парола за настройки. Паролата за настройки предотвратява неоторизираният достъп до Computer Setup (Настройка на компютъра).

Ключалката на интелигентния капак е налична при определени системи.

Заключване на ключалката на интелигентния капак

За да активирате и заключите тази ключалка, изпъкнете следните стъпки:

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Restart (Рестартиране)**.
2. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

---

3. Изберете опцията **Security (Защита) > Smart Cover (Интелигентен капак) > Cover Lock (Ключалка на капака) > Lock (Заключване)**.
4. Преди да излезете, щракнете върху **File (Файл) > Save Changes and Exit (Запис на настройките и изход)**.

Отключване на ключалката на интелигентния капак

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Restart (Рестартиране)**.
2. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

3. Изберете **Security (Защита) > Smart Cover (Интелигентен капак) > Cover Lock (Ключалка на капака) > Unlock (Отключване)**.
4. Преди да излезете, щракнете върху **File (Файл) > Save Changes and Exit (Запис на настройките и изход)**.

Използване на ключа FailSafe на интелигентния капак

Ако активирате ключалката на интелигентния капак и не можете да въведете паролата, за да я деактивирате, ще ви трябва ключ FailSafe за интелигентния капак, за да го отворите. Този ключ ще ви трябва в следните случаи:

- Прекъсване на електрозахранването
- Неуспешно начално стартиране
- Повреда на компютърен компонент (напр. процесор или захранване)
- Забравена парола

ВНИМАНИЕ: Ключът FailSafe е специализиран инструмент от HP. Подгответе се; поръчайте този ключ преди да ви потрябва от оторизиран риселър или сервиз.

За да получите ключа FailSafe, направете едно от следните неща:

- Обърнете се към оторизиран риселър или сервиз на HP.
- Обадете се на съответния телефонен номер от гаранцията.

За повече информация за използването на ключа FailSafe на интелигентния капак, вж. *Hardware Reference Guide (Ръководство за справки по хардуера)* на *Documentation CD (Компактдиск с документация)*.

Master Boot Record Security (Защита на главния сектор за стартиране)

Главният сектор за стартиране (MBR) съдържа информация за успешното стартиране от диск и за достъп до данните на диска. Защитата на главния сектор за стартиране открива и отчита неумишлени и умишлени промени в MBR, като например от вируси или неправилна употреба на някои дискови програми. Тя също позволява да се възстанови «последния правилен» сектор, ако случайно има промени в него при рестартиране на системата.

За да разрешите защитата на сектора за начално стартиране, изпълнете следните стъпки:

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Restart (Рестартиране)**.
2. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

---

3. Изберете **Security (Защита) > Master Boot Record Security (Защита на главния сектор за стартиране) > Enabled (Разрешен)**.
4. Изберете **Security (Защита) > Save Master Boot Record (Запиши главния сектор за стартиране)**.
5. Преди да излезете, щракнете върху **File (Файл) > Save Changes and Exit (Запис на настройките и изход)**.

Когато защитата на главния сектор за защита е активирана, BIOS не допуска промени в сектора на текущо стартиращия диск в режим MS–DOS и безопасен режим на Windows.

Повечето операционни системи контролират достъпа до главния сектор за стартиране; BIOS не може да предотврати промените, направени по време на изпълнението на операционната система.

При всяко включване или рестартиране на компютъра, BIOS сравнява MBR сектора на текущия стартиращ диск с този, който е записан преди това. Ако има промени и ако текущият стартиращ диск е този, от който секторът е бил записан, ще се покаже следното съобщение:

1999—Master Boot Record has changed
(Има промени в главния сектор за стартиране).

Натиснете произволен клавиш, за да влезете в настройките и конфигурирате защитата на главния сектор за стартиране.

При влизане в Computer Setup (Настройка на компютъра), трябва да

- Запишете MBR сектора на текущия стартиращ диск;
- Възстановите вече записания MBR сектор или;
- Забраните функцията за защита на MBR сектора.

Трябва да знаете паролата за настройки, ако има такава.

Ако има промени и ако текущият стартиращ диск **не** е този, от който секторът е бил записан, ще се покаже следното съобщение:

2000—Master Boot Record Hard Drive has changed
(Има промени в твърдия диск, където е главния сектор за стартиране).

Натиснете произволен клавиш, за да влезете в настройките и конфигурирате защитата на главния сектор за стартиране.

При влизане в Computer Setup (Настройка на компютъра), трябва да

- Запишете MBR сектора на текущия стартиращ диск или;
- Забраните функцията за защита на MBR сектора.

Трябва да знаете паролата за настройки, ако има такава.

Ако случайно записаният MBR сектор е повреден, ще се появи следното съобщение:

1998—Master Boot Record has been lost
(Изтрит е главния сектор за стартиране).

Натиснете произволен клавиш, за да влезете в настройките и конфигурирате защитата на главния сектор за стартиране.

При влизане в Computer Setup (Настройка на компютъра), трябва да

- Запишете MBR сектора на текущия стартиращ диск или;
- Забраните функцията за защита на MBR сектора.

Трябва да знаете паролата за настройки, ако има такава.

Преди да разделите на дялове или форматирате текущия стартиращ твърд диск

Уверете се, че защитата на MBR сектора е забранена, преди да промените дяловете или форматирате текущия стартиращ диск. Няколко помощни дискови програми, като FDISK и FORMAT, искат достъп за промяна на MBR сектора. Ако е разрешена защитата на MBR сектора при разделянето на дялове или форматирането на диска, може да се появят съобщения за грешка от помощната програма или предупреждение от защитата на MBR сектора при следващото включване или рестартиране на компютъра. За да разрешите защитата на главния сектор за стартиране, изпълнете следните стъпки:

1. Включете или рестартирайте компютъра. Ако сте в Windows, щракнете върху **Start (Старт) > Shut Down (Изключване) > Restart (Рестартиране)**.
2. Веднага щом компютърът се включи, натиснете и задръжте клавиша **F10**, за да влезете в Computer Setup. Натиснете клавиша **Enter**, за да прескочите заглавния екран, ако е нужно.

Ако не успеете да натиснете клавиша **F10** в подходящия момент, ще трябва да рестартирате компютъра и отново да натиснете и задържите клавиша **F10**, за да влезете в помощната програма.

Ако използвате PS/2 клавиатура, може да се появи съобщение за грешка на клавиатурата – игнорирайте го.

---

3. Изберете **Security (Защита) > Master Boot Record Security (Защита на главния сектор за стартиране) > Disabled (Забранен)**.
4. Преди да излезете, щракнете върху **File (Файл) > Save Changes and Exit (Запис на настройките и изход)**.

Наличие на кабелна ключалка

На задния панел на компютъра се намира кабелна ключалка, чрез която компютърът може физически да се прикрепи към работно място.

За инструкции с илюстрации, вж. *Hardware Reference Guide (Ръководство за справки по хардуера)* в *Documentation CD (Компактдиск с документация)*.

Технология за идентифициране по отпечатъци на пръсти

Елиминирайки нуждата от въвеждането на потребителски пароли, технологията за идентифициране по отпечатъци на пръсти на HP увеличава мрежовата сигурност, опростява процеса на регистриране и намалява разходите за управление на корпоративните мрежи. Технологията е ценово достъпна и вече не е само за високотехнологични организации с голямо ниво на защита.

Поддръжката на технологията за идентифициране по отпечатъци на пръстите е различна според модела.

За още информация посетете:

http://h18004.www1.hp.com/products/security/.

Уведомяване при грешки и възстановяване

Функциите за уведомяване при грешки и възстановяване комбинират нови хардуерни и софтуерни технологии, за да предотвратят загубата на критично важни данни и да намалят непланирания престой на системите.

Ако компютърът е свързан към мрежа, която се управлява от HP Client Manager, той изпраща съобщение за грешка на приложението за управление на мрежата. С HP Client Manager Software можете също така отдалеч да планирате автоматичното изпълнение на диагностика на всички управляеми компютри и да генерирате отчет на неуспешните тестове.

Система за защита на устройства

Системата за защита на устройства (DPS) е инструмент за диагностика, вграден в твърди дискове, инсталирани в определени компютри на HP. DPS е проектирана да помага при диагностиката на проблемите, които могат да доведат до замяна на твърдите дискове.

При асемблирането на компютрите на HP всеки твърд диск се тества с DPS като се записва постоянно информация. При всяко изпълнение на DPS системата, резултатите от теста се записват на твърдия диск. Тази информация може да се използва от сервиза при диагностиката на проблемите, които са довели до изпълнението на софтуера DPS. Вж. *Troubleshooting Guide (Ръководство за отстраняване на неизправности)* в *Documentation CD (Компактдиск с документация)* за повече информация за използването на DPS.

Захранване, устойчиво на токови удари

Вграденото захранване, защитено срещу токови удари, предоставя по–голяма надеждност при евентуални токови удари. Това захранване може да издържи токов удар от 2000 волта без да се наруши работата на системата или да се загубят данни.

Сензор за температура

Сензорът за температура е хардуерна и софтуерна функция, която следи вътрешната температура на компютъра. Тази функция показва предупредително съобщение при нарушение на нормалния диапазон, което ви дава време да предприемете мерки преди вътрешните компоненти да се повредят или да се загубят данни.

Индекс

A-Z

Б

В

Д

З

И

К

Н

О

П

Р

С

Т

У

Ф